AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with the five MeWe accounts detailed in Attachment A-1

Case No. 3:20 mj 039

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A-1

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
See Attachment C-1	

The application is based on these facts:
See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig
Applicant's signature

Andrea R. Kinzig, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 1-22-20

Sharon L. Ovington
Judge's signature

City and state: Dayton, Ohio

Sharon L. Ovington, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A-1

Property to Be Searched

Information associated with the following MeWe accounts that is stored at premises owned, maintained, controlled, or operated by Sgrouples Inc., doing business as (dba) MeWe, a company that accepts service of legal process at 801 California Street, Mountain View, California, 94041:

MeWe User ID	MeWe User Name:	Associated Email Address:
5d80ca7e8deabf7250fbfe3e	Juan Lesstime	tj599427@gmail.com
5d95dd51182b702cccb57ddd	Juan Goodtime	js0867517@gmail.com
5da84d7ef9c09b69a959c8ea	Juan Twothree	tt4883957@gmail.com
5dcd56c37c698c685e8130ab	David Dickson	daviddickson335@gmail.com
5de10e4281b61c103a6639f3	Dave Jackson	dave72042@gmail.com

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by Sgrouples Inc. (the "Provider")

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the Provider, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each user ID listed in Attachment A-1:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, passwords, security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other MeWe activities.

(c) All photographs and videos uploaded by the user and all photographs and videos uploaded by any other user that have the user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photographs and videos.

(d) All profile information; timeline information; videos, photographs, articles, and other items; all Contact lists, including the Contacts' MeWe user identification numbers; groups and networks of which the user is a member, including the groups' MeWe group identification numbers; future and past event postings; rejected Contact requests; comments; tags; and other information about the user's access and use of MeWe applications.

(e) All records or other information regarding the devices and Internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string.

(f) All other records and contents of communications and messages made or received by the user, including all chat communication activities, private messages, chat histories, video and voice calling histories, and pending "Contact" requests.

(g) All IP logs, including all records of the IP addresses that logged into the account.

(h) All records of the account's feedback to MeWe posts.

(i) All information about the MeWe pages that the account followed.

(j) All past and present lists of Contacts created by the account.

(k) All records of MeWe searches performed by the account.

(l) The length of service (including start date), the type of services utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number).

(m) All privacy settings and other account settings, including privacy settings for individual MeWe posts and activities.

(n) All records pertaining to communications between MeWe and any person regarding the user or the user's MeWe account, including contacts with support services and records of actions taken.

(o) Any other MeWe accounts associated with the listed accounts by cookies, recovery email address, or telephone number.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant. Notwithstanding 18 U.S.C. § 2252/2252A or any similar statute or code, the Provider shall disclose responsive data by sending it to the Federal Bureau of Investigation at 7747 Clyo Road, Centerville, Ohio, 45459.

II. Information to be seized by the government

Items evidencing violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession of child pornography); and 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography); from January 1, 2019 through the present, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and distribution of child pornography.

2. Any visual depictions of minors, and any identifying information for these minors.

3. Any communications with others in which child exploitation materials and offenses are discussed and/or traded.

4. Any communications with minors, and any identifying information for these minors.

5. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.

6. Evidence of utilization of telephone accounts;

7. Any information related to Internet Protocol (IP) addresses accounts accessed by the accounts.

8. Any information related to the use of aliases.

9. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-1

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt and Distribution of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.

2. Along with other agents, officers, and investigators of the FBI, I am currently involved in an investigation of child pornography offenses committed by an individual utilizing the user names of David Dixon, David Dickson, David Jackson, Juan Lesstime, Juan Goodtime, and Juan Twothree on email and social media applications. This Affidavit is submitted in support of Applications for search warrants for the following:

   a. Information associated with the MeWe accounts associated with the email addresses **daviddickson335@gmail.com**, **dave72042@gmail.com**, **tj599427@gmail.com**, **js0867517@gmail.com**, and **tt4883957@gmail.com** that is stored at premises controlled by Sgrouples Inc., doing business as (dba) MeWe (as more fully described in Attachment A-1), and

   b. Information associated with the Google accounts **southernman4501@gmail.com**, **daviddickson335@gmail.com**, **dave72042@gmail.com**, **tj599427@gmail.com**, **js0867517@gmail.com**, and **tt4883957@gmail.com** that is stored at premises controlled by Google LLC (as more fully described in Attachment A-2).

3. The purpose of the Applications is to seize evidence of violations of the following:

   a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess child pornography; and

   b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce.

4. The items to be searched for and seized are described more particularly in Attachments B-1 and B-2 hereto and are incorporated by reference.

5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the above noted accounts (as described in Attachments A-1 and A-2).

7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law; including violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1), are present in the information associated with the above noted accounts (as described in Attachments A-1 and A-2).

JURISDICTION

8. This court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL CRIMINAL STATUTES

9. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

10. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign

commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

11. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

12. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

Definitions

13. The following definitions apply to this Affidavit and Attachments B-1 and B-2 to this Affidavit:

a. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. "**Minor**" means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. §§ 2256(2) and 1466A(f)).

e. An "**Internet Protocol address**", also referred to as an "**IP address**", is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

f. "**Hyperlink**" (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

g. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

h. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer

on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

i. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Background on Computers and Child Pornography

14. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

15. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

16. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or

through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

17. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

18. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

19. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

20. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Collectors of Child Pornography

21. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):

a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

d. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Google Services

22. Google LLC is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.

23. Google Photos is a photograph and video sharing and storage service provided by Google LLC, located at photos.google.com. It allows users to back-up their photographs and videos so they can be accessed on any telephone, tablet, or computer. It also allows users to pool their photographs and videos together with others into shared albums. Photographs and videos can be organized and searched by places and things in them.

24. Google+ is a social networking and identity service website owned and operated by Google LLC, located at www.plus.google.com. Common features include the following:

a. Profiles: Users can establish profile pages to maintain personal information, similar to the Facebook and MySpace social networking sites.

b. Circles: Google+ allows users to establish "circles", which enables them to organize people into groups for sharing across various Google products and services. This service replaces the typical "Friends" list function used by sites such as Facebook and MySpace.

c. Communities: Communities allow users with common interests to communicate with each other.

d. Photos: Google+ allows users to post, back-up, and share photographs. Users can also make comments on photographs posted by other users.

e. Hangouts: Hangouts are places used to facilitate group video chat. Only Google+ users can join such chats.

f. Messenger: Messenger is a feature available to Android, iPhone, and SMS devices for communicating through instant messaging within Circles.

25. Google Web and App History is a feature of Google Search in which a user's search queries and results and activities on other Google services are recorded. The feature is only available for users logged into a Google account. A user's Web and App History is used to personalize search results with the help of Google Personalized Search and Google Now.

26. Google Drive is a file storage and synchronization service provided by Google LLC, located at www.drive.google.com. This service provides cloud storage, file sharing, and collaborative editing capabilities. It offers 15 GB of online storage space, which is usable across Google Drive, Gmail, and other Google services.

27. Google Android Backup is a service provided by Google LLC to backup data connected to users' Google accounts. The service allows users to restore data from any Google account that has been backed up in the event that the users' devices are replaced or erased. Data that can be backed up includes Google Calendar settings, WiFi networks and passwords, home screen wallpapers, Gmail settings, applications installed through Google Play, display settings, language and input settings, date and time, and third party application settings and data.

Email Accounts

28. Google LLC allows subscribers to obtain email accounts at the domain name gmail.com, like the accounts listed in Attachment A-2. Subscribers obtain accounts by registering with Google LLC. During the registration process, Google LLC asks subscribers to provide basic personal information. Therefore, the computers of Google LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google LLC subscribers) and information concerning subscribers and their use of Google LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

29. In general, an email that is sent to a Google LLC subscriber is stored in the subscriber's "mail box" on Google LLC's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google LLC's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google LLC's servers for a certain period of time.

30. Google LLC subscribers can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google LLC. In my

training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

31. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

32. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

33. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

34. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For

example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

MeWe

35. Sgrouples Inc., dba MeWe, is a company based in Mountain View, California. Sgrouples Inc. owns and operates the MeWe website, which is a free-access social networking website that can be accessed at http://mewe.com. MeWe allows its users to establish accounts with MeWe, and users can then use their accounts to share photographs, videos, documents, voice messages, chats, GIFS[1], memes[2], and other information with other MeWe users. MeWe users can see posts, chats, comments, etc. made by individuals, pages, and groups with whom they are connected.

36. MeWe asks its users to provide basic contact and personal identifying information, either during the registration process or thereafter. This information may include the user's full name, date of birth, gender, contact e-mail address, MeWe passwords, physical address, telephone numbers, screen names, websites, and other personal identifiers. MeWe also assigns a user identification number to each account.

37. MeWe users may join one or more groups or networks to connect and interact with other users. MeWe assigns a group identification number to each group. A MeWe user can also connect directly with individual MeWe users by sending a "Contact Request". If the recipient of a "Contact Request" accepts the request, then the two users will become "Contacts" for purposes of MeWe and can exchange communications or view

1 A GIF is an image that has been encoded using the graphics interchange format, where it has multiple frames encoded into a single image file. A web browser or other software will play those images back in an animated sequence automatically.

2 A meme is an idea, behavior, or style that spreads by means of imitation from person to person within a culture – often with the aim of conveying a particular phenomenon, theme, or meaning represented by the meme. An Internet meme is a type of meme which is spread, often through social media platforms, via the Internet.

information about each other. Each MeWe user's account includes a list of that user's "Contacts".

38. MeWe users can select different levels of privacy for their communications and the information associated with their MeWe accounts. By adjusting these privacy settings, a MeWe user can make information available only to himself or herself or to particular MeWe users. A MeWe user can also create "lists" of MeWe contacts to facilitate the application of these privacy settings. MeWe accounts also include other account settings that users can adjust, such as the types of notifications they receive from MeWe.

39. MeWe users can create profiles that include photographs, lists of personal interests, and other information. MeWe users can also post links to videos, photographs, articles, and other items available elsewhere on the Internet. MeWe users can post information about upcoming "events", such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Timeline", which is a space where the user and his or her "Contacts" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

40. MeWe allows users to upload photographs and videos to their accounts. These files may include metadata such as the user's location when he or she uploaded the photographs and videos. MeWe also provides users with the ability to "tag" (i.e., label) other MeWe users in photographs and videos. When a user is tagged in a photograph or video, he or she receives a notification of the tag and a link to see the photograph or video. For MeWe's purposes, the photographs and videos associated with a user's account will include all photographs and videos uploaded by that user that have not been deleted, as well as all photographs and videos uploaded by any other user that have that user tagged in them.

41. MeWe users can exchange private messages on MeWe with other users. These messages are stored by MeWe unless deleted by the user. MeWe users can also post comments on the MeWe profiles of other users or on their own profiles, and such comments are typically associated with a specific posting or item on the profile.

42. If a MeWe user does not want to interact with another user on MeWe, the first user can "block" the second user from seeing his or her account.

43. MeWe allows users to give positive feedback or connect to particular pages. MeWe users can also follow particular MeWe pages.

44. MeWe has a search function that enables its users to search MeWe for keywords, usernames, or pages, among other things.

45. MeWe retains IP logs for a given user ID or IP address for 30 days. These logs may contain information about the actions taken by the user ID or IP address on MeWe,

including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a MeWe profile, that user's IP log would reflect the fact that the user viewed the profile and would show when and from what IP address the user did so.

46. Social networking providers such as MeWe typically retain additional information about their users' accounts, such as information about the length of service (including start dates), the type of services utilized, and the means and source of any payments associated with the service (including any credit card or bank account numbers). In some cases, MeWe users may communicate directly with MeWe about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers such as MeWe typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

47. MeWe maintains records that may reveal other accounts accessed from the same electronic device, such as the same computer or mobile phone, and accounts that are linked by "cookies" (small pieces of text sent to the user's Internet browser when visiting websites).

48. The computers of MeWe are likely to contain all of the material detailed above, including stored electronic communications and information concerning subscribers and their use of MeWe, such as account access information, transaction information, and account application.

NCMEC and Cyber Tipline Reports

49. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.

50. As part of its functions, NCMEC administers the Cyber Tipline. The Cyber Tipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the Cyber Tipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities.

FACTS SUPPORTING PROBABLE CAUSE

Cyber Tipline Reports from MeWe

51. As part of the investigation, I have learned that MeWe filed approximately five reports to NCMEC's Cyber Tipline regarding suspected child pornography or child exploitation files that were located in five separate MeWe accounts, all of which utilized the IP address of 98.29.147.70 to access the accounts. Four of the five MeWe accounts also utilized the IP address of 107.77.193.231. These five reports were made during the approximate time period September 2019 through November 2019.

52. In its reports, MeWe reported that a total of approximately one hundred seventy-two (172) suspected child pornography or child exploitation files had been located in the five accounts. MeWe provided these files to NCMEC as part of its Cyber Tipline reports.

53. NCMEC forwarded MeWe's five Cyber Tipline reports, along with the suspected child pornography or child exploitation files, to the Ohio Internet Crimes Against Children Task Force (ICAC) for further investigation. I have obtained and reviewed MeWe's Cyber Tipline reports and the accompanying files from the Cuyahoga County ICAC as part of the investigation. Based on my review of the files and my training and experience, I believe that at least approximately one hundred twenty-eight (128) of the one hundred seventy-two (172) files depict child pornography. Below is a summary of the Cyber Tipline Reports:

a. On or around October 31, 2019, MeWe reported to NCMEC's Cyber Tipline that the company had discovered approximately forty-one (41) suspected child pornography or child exploitation files in a MeWe account that had utilized the IP address of 98.29.147.70. This account had a user name of "Juan Lesstime" and was associated with the email address of **tj599427@gmail.com**. In addition to the IP address of 98.29.147.70, the IP address of 107.77.193.231 had also been utilized to access the account. Based on my review of the files and my training and experience, I believe that approximately thirty-four (34) of the files submitted by MeWe depict child pornography. By way of example, one of these files is described as follows:

i. Screenshot_2019-08-01-07-38-56~2.png: The file is an image that depicts what appears to be an adult white male (whose face is not captured in the image) ejaculating into the mouth of a pre-pubescent white female child.

b. On or around October 31, 2019, MeWe reported to NCMEC's Cyber Tipline that the company had discovered approximately fifty-nine (59) suspected child pornography or child exploitation files in a MeWe account that had utilized the IP address of 98.29.147.70. The account had a user name of "Juan Goodtime" and

was associated with the email address of **js0867517@gmail.com**. In addition to the IP address of 98.29.147.70, the IP addresses of 107.77.193.231, 75.186.53.96, and 166.216.159.66 had also been utilized to access the account. Based on my review of the files and my training and experience, I believe that approximately thirty-two (32) of the files submitted by MeWe depict child pornography. By way of example, one of these files is described as follows:

i. 158408250_2570aea8-d7d3-4d13-8f65-d9b537d3e974.jpg: The file is an image that depicts what appears to be a nude pre-pubescent white male child lying on a bed. What appears to be an adult female is performing fellatio on the child's penis.

c. On or around November 7, 2019, MeWe reported to NCMEC's Cyber Tipline that the company had discovered approximately fifty-one (51) suspected child pornography or child exploitation files in a MeWe account that had utilized the IP address of 98.29.147.70. This account had a user name of "Juan Twothree" and was associated with the email address of **tt4883957@gmail.com**. In addition to the IP address of 98.29.147.70, the IP addresses of 107.77.193.231, 75.186.53.96, 166.216.159.66, and 68.45.76.39 had also been utilized to access the account. Based on my review of the files and my training and experience, I believe that approximately forty-five (45) of the files submitted by MeWe depict child pornography. By way of example, one of these files is described as follows:

i. 159802708_iOS_image_upload%20(53).jpg: The file is an image that depicts a close-up of the nude vagina and anus of what appears to be a pre-pubescent white female child. What appears to be a penis is inserted into the child's anus.

d. On or around November 26, 2019, MeWe reported to NCMEC's Cyber Tipline that the company had discovered approximately nineteen (19) suspected child pornography or child exploitation files in a MeWe account that had utilized the IP address of 98.29.147.70. The account had a user name of "David Dickson" and was associated with the email address of **daviddickson335@gmail.com**. In addition to the IP address of 98.29.147.70, the IP address of 75.186.53.96 had also been utilized to access the account. Based on my review of the files and my training and experience, I believe that approximately sixteen (16) of the files submitted by MeWe depict child pornography. By way of example, one of these files is described as follows:

i. 1415603038-VID_20141109_234029.mp4: The file is a video that depicts a nude pre-pubescent white female child lying on a bed with her legs straddled. What appears to be an adult white male (whose face is not captured in the image) masturbates his penis over the child. He then partially inserts his penis into the child's vagina and ejaculates onto her

vagina. The video is approximately fifty-nine (59) seconds in duration.

e. On or around December 2, 2019, MeWe reported to NCMEC's Cyber Tipline that the company had discovered approximately two suspected child pornography or child exploitation files in a MeWe account that had utilized the IP address of 98.29.147.70. The account had a user name of "David Jackson" and was associated with the email address of **dave72042@gmail.com**. In addition to the IP address of 98.29.147.70, the IP address of 107.77.193.231 had also been utilized to access the account. Based on my review of the files and my training and experience, I believe that approximately one of the files submitted by MeWe depicts child pornography. This file is described as follows:

i. Image(501).jpg: The file is an image that depicts a nude pre-pubescent white female child sitting on a couch with her legs straddled, exposing her nude vagina to the camera.

Google LLC Cyber Tipline Reports

54. As part of the investigation, I have learned that Google LLC filed approximately seven Cyber Tipline reports regarding suspected child pornography or child exploitation files located in a Google account that had utilized the IP addresses of 98.29.147.70 and 107.77.193.231 to access the account (the same IP addresses utilized to access the above noted MeWe accounts). This Google account was associated with the email address of **southernman4501@gmail.com** and the telephone number 240-609-9375. These seven reports were made in or around November 2019. Each of the reports noted that the suspected child pornography or child exploitation files were located in the Google Photos account associated with the **southernman4501@gmail.com** email address.

55. In its reports, Google LLC reported that a total of approximately nine suspected child pornography or child exploitation files had been located in the Google Photos account associated with the **southernman4501@gmail.com** email address. Google LLC provided these files to NCMEC as part of its Cyber Tipline reports.

56. NCMEC forwarded Google LLC's seven Cyber Tipline reports, along with the suspected child pornography or child exploitation files, to the Ohio ICAC for further investigation. I have obtained and reviewed Google LLC's Cyber Tipline reports and the accompanying files from the Cuyahoga County ICAC as part of the investigation. Based on my review of the files and my training and experience, I believe that at least approximately seven of the nine files depict child pornography. By way of example, two of these files are described as follows:

a. 2019-11-11.png: The file is an image that depicts what appears to be a nude pre-pubescent white female child who is kneeling on a bed. What appears to be a nude adult white male is kneeling behind the child and inserting his penis into the

child's anus or vagina. This file was reported by Google LLC to NCMEC's Cyber Tipline on or around November 14, 2019.

b. 2019-11-11.png: The file is an image that depicts what appears to be a nude pre-pubescent white male child standing in a bedroom. What appears to be a nude pre-pubescent white female child is sitting on the floor in front of the male child, and she is performing fellatio of the male child's penis. This file was reported by Google LLC to NCMEC's Cyber Tipline on or around November 20, 2019.

Results of Subpoenas

57. AT&T was identified as the service provider for telephone number 240-609-9375 (the telephone number associated with the **southernman4501@gmail.com** account). On or around January 8, 2020, an FBI investigator served an administrative subpoena to AT&T requesting subscriber information for this telephone number. Records received in response to the subpoena identified that the telephone number was a pre-paid account, and that no subscriber information was maintained by AT&T for the account user.

58. Charter Communications was identified as the Internet Service Provider for the IP address of 98.29.147.70 (one of the IP addresses utilized to access the MeWe and Google accounts detailed above). On or around December 6, 2019, an investigator from the Cuyahoga County ICAC served an administrative subpoena to Charter Communications requesting subscriber information for this IP address on one of the dates and times that it was used to access one of the MeWe accounts. Records received in response to the subpoena identified that this IP address was subscribed to Richard Weller at 120 Sandhurst Street in Verona, Ohio. Records identified that this Internet account was activated on or around September 15, 2011.

59. AT&T Mobility was identified as the Internet Service Provider for the IP address of 107.77.193.231 (another one of the IP addresses utilized to access the MeWe and Google accounts detailed above). The use of an IP address serviced by AT&T Mobility is consistent with someone using his or her cellular telephone's data plan to access the Internet. As detailed above, AT&T was identified as the service provider for telephone number 240-609-9375. As such, it is reasonable to believe that a cellular telephone was utilized to access the MeWe and Google accounts detailed above on some occasions.

60. On or around January 16, 2020, an administrative subpoena was served to Sgrouples Inc. requesting subscriber information and logs of IP addresses for the MeWe accounts associated with the email addresses of **daviddickson335@gmail.com**, **dave72042@gmail.com**, **tj599427@gmail.com**, **js0867517@gmail.com**, and **tt4883957@gmail.com**. Records received in response to the subpoena provided the following information:

a. The account associated with the email address of **tj599427@gmail.com** had a

MeWe user name of Juan Lesstime and a MeWe User ID of 5d80ca7e8deabf7250fbfe3e. The account was registered on or around September 17, 2019.

b. The account associated with the email address **js0867517@gmail.com** had a MeWe User name of Juan Goodtime and a MeWe User ID of 5d95dd51182b702cccb57ddd. The account was registered on or around October 3, 2019.

c. The account associated with the email address **tt4883957@gmail.com** had a MeWe User name of Juan Twothree and a MeWe User ID of 5da84d7ef9c09b69a959c8ea. The account was registered on or around October 17, 2019.

d. The account associated with the email address **daviddickson335@gmail.com** had a MeWe User name of David Dickson and a MeWe User ID of 5dcd56c37c698c685e8130ab. The account was registered on or around November 14, 2019.

e. The account associated with the email address **dave72042@gmail.com** had a MeWe User name of Dave Jackson and a MeWe User ID of 5de10e4281b61c103a6639f3. The account was registered on or around November 29, 2019.

61. Review of records from the Ohio Bureau of Motor Vehicles identified that Richard Weller and three other individuals utilized the address of 120 Sandhurst Street in Verona, Ohio on their current Ohio driver's licenses. The true identity of the user(s) of the MeWe and Google accounts detailed above is not known at this time.

Evidence Available in Email and Social Media Accounts

62. Based on my training and experience, I am aware that individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

63. Also in my experience, individuals involved in child exploitation schemes often utilize email, social media, and online chat programs as a means to locate and recruit victims. They then use the chat functions on these and other websites, as well as email accounts,

to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.

64. Based on my training and experience, I know that individuals involved in child pornography offenses often obtain and trade images with each other via a variety of means, including email, social media accounts, photo sharing services, and online chat programs. Individuals also often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, Internet bulletin boards, Internet Peer-to-Peer file sharing programs, Internet websites, and other sources. I have also seen a number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.

65. Based on my training and experience, one or more aliases are often used by individuals involved in child exploitation offenses as a means to avoid detection from law enforcement. It is not uncommon for such offenders to create multiple identities, sometimes involving different ages and genders. Offenders sometimes fictitiously portray themselves as juveniles as a means to gain trust and rapport with victims. Offenders also sometimes obtain photographs of other individuals from the Internet to use as their profile pictures and/or to send to the victims.

66. Based on my training and experience, I know that many social media accounts, Internet websites, and telephone providers require users to provide their email accounts when registering for the accounts. The social media and Internet account providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. Telephone providers often send bills to their customers via email. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media, Internet accounts, and telephone account that were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.

67. Also as noted above, email providers maintain various subscriber and user information that their users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized to trade child pornography, as this information can help in confirming the identities of the individuals using the accounts and committing the offenses.

68. Furthermore, any communications to or from the aforesaid email accounts (including communications with adults or other third parties) may be materially relevant to the

investigation, as these communications may help to corroborate the identity of the MeWe and Google account user.

69. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Sought in Other Google Accounts

70. Google LLC has the ability to maintain information associated with the Web and Application history of its users. Such information is materially relevant in child exploitation investigations, as it may help in identifying websites used by subjects to obtain child pornography and locate victims.

71. Google Drive and Google Photos provide users with cloud computing and online file storage (as detailed above) and photo storage services. In my experience, individuals with large collections of child pornography may utilize cloud computing and online storage accounts as a means to store their files after their hard drives become full. In addition, individuals utilize these services as a means to conceal their files from others, including law enforcement.

72. Google Android Backup provides users with the ability to backup data on their cellular telephones and other electronic devices. Such data can be materially relevant in cases in which cellular telephones and other electronic devices are used to commit child exploitation offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.

Conclusion Regarding Use of Accounts:

73. Based on all of the information detailed above, there is probable cause to believe that the MeWe accounts associated with the email addresses **daviddickson335@gmail.com**, **dave72042@gmail.com**, **tj599427@gmail.com**, **js0867517@gmail.com**, and **tt4883957@gmail.com** contain evidence of the possession and receipt of child pornography. There is also probable cause to believe that the Google Photos account associated with the email address of **southernman4501@gmail.com** contains evidence of the possession and receipt of child pornography.

74. Also based on the information detailed above, there is probable cause to believe that information related to any Google accounts associated with the **daviddickson335@gmail.com**, **dave72042@gmail.com**, **tj599427@gmail.com**, **js0867517@gmail.com**, **tt4883957@gmail.com**, and **southernman4501@gmail.com** email addresses (including contents of email accounts, Web and App history data,

contents of Google Photos and Google Drive accounts, and contents of Google+ accounts) may contain material evidence regarding the account user's child pornography activities and/or the account user's identity.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

75. I anticipate executing the requested warrants for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Sgrouples Inc. and Google LLC to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachments B-1 and B-2. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2.

CONCLUSION

76. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law; including violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1), are present in the information associated with the above noted accounts (as described in Attachments A-1 and A-2).

77. I, therefore, respectfully request that the attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 and B-2.

78. Because the warrants for the accounts described in Attachments A-1 and A-2 will be served on Sgrouples Inc. and Google LLC, who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

Andrea R. Kinzig

Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 22nd of January 2020

Sharon L. Ovington

SHARON L. OVINGTON
UNITED STATES MAGISTRATE COURT JUDGE